

November 25, 2002



Information System Security

Government Information Security
Reform Act Implementation:
Defense Advanced Research
Projects Agency Management
Support System
(D-2003-027)

Department of Defense
Office of the Inspector General

Quality

Integrity

Accountability

Report Documentation Page

Report Date 25 Nov 2002	Report Type N/A	Dates Covered (from... to) -
Title and Subtitle Information System Security: Government Information Security Reform Act Implementation: Defense Advanced Research Projects Agency Management Support System		Contract Number
		Grant Number
		Program Element Number
Author(s)		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es) OAIG-AUD (ATTN: AFTS Audit Suggestions) Inspector General Department of Defense 400 Army Navy Drive (Room 801) Arlington, VA 22202-2884		Performing Organization Report Number D-2003-027
Sponsoring/Monitoring Agency Name(s) and Address(es)		Sponsor/Monitor's Acronym(s)
		Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms		
Report Classification unclassified	Classification of this page unclassified	
Classification of Abstract unclassified	Limitation of Abstract UU	
Number of Pages 60		

Additional Copies

To obtain additional copies of this report, visit the Web site of the Inspector General of the Department of Defense at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General of the Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ASD(C ³ I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
DAA	Designated Approving Authority
DARPA	Defense Advanced Research Projects Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMSS	Defense Advanced Research Projects Agency Management Support System
GISR	Government Information Security Reform
SSAA	System Security Authorization Agreement



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

November 25, 2002

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND,
CONTROL, COMMUNICATIONS, AND INTELLIGENCE)
DIRECTOR, DEFENSE ADVANCED RESEARCH PROJECTS
AGENCY

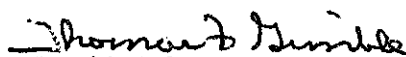
SUBJECT: Report on Government Information Security Reform Act Implementation:
Defense Advanced Research Projects Agency Management Support System
(Report No. D-2003-027)

We are providing this report for review and comment. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. Defense Advanced Research Projects Agency comments were not responsive; we request additional comments on the recommendations by January 24, 2003.

If possible, please provide management comments in electronic format (Adobe Acrobat file only). Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Mr. Tilghman A. Schraden at (703) 604-9186 (DSN 664-9186) or Ms. Kathryn L. Palmer at (703) 604-8840 (DSN 664-8840). See Appendix D for the report distribution. Audit team members are listed inside the back cover.


for David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General of the Department of Defense

Report No. D-2003-027

(Project No. D2002LD-0101)

November 25, 2002

Government Information Security Reform Act Implementation: Defense Advanced Research Projects Agency Management Support System

Executive Summary

Who Should Read This Report and Why? DoD personnel who are involved in implementing Government Information Security Reform Act (GISR Act) requirements should read this report. The report discusses our independent assessment of the information security posture of the Defense Advanced Research Projects Agency (DARPA) Management Support System, a DARPA system.

Background. To gather data on assessments of the effectiveness of DoD information assurance policies, procedures, and practices, DoD developed a GISR Act collection matrix for automated information systems. DoD selected a sample of 560 automated information systems from the almost 4,000 automated information systems in DoD. For those 560 systems, DoD reported the aggregate results of the assessments for FY 2001 in "GISR Report FY01: Government Information Security Reform Act, Report of the Department of Defense," October 2001. Of the 560 systems, the Office of the Inspector General of the Department of Defense, the Defense Information Systems Agency Inspector General, and Military Department audit agencies assessed a sample of 115 systems. This report is one in a series of GISR Act audits and is an assessment of the DARPA Management Support System. The DARPA Management Support System is a mission-essential system that supports DARPA and its various technical and support offices.

Results. The data reported for the DARPA Management Support System in the GISR Act collection matrix for FY 2001 were partially inaccurate as of August 1, 2001, the date of the FY 2001 collection matrix data. DARPA answered 5 of the 32 collection matrix data fields incorrectly. Also, DARPA did not provide documentation that supported 8 of the 32 responses. Additionally, the key DARPA information assurance staff positions were not aligned in a way that ensures segregation of duties and the required checks and balances in the DoD Information Technology Security Certification and Accreditation Process for the DARPA Management Support System. Furthermore, DARPA did not formally appoint three of the four key information assurance staff positions required to ensure the appropriate checks and balances during the certification process. Also, the designated approving authority was not within the operational chain of command, as the DoD Information Technology Security Certification and Accreditation Process requires. Further, DARPA did not provide support that it had verified that the contractors working on the system had proper security clearances. As a result, the DARPA Management Support System may not have adequate information security operational controls that ensure sensitive information is safeguarded. For details of the audit results, see the Finding section of the report.

Management Comments and Audit Response. DARPA nonconcurred with the finding and the recommendations. DARPA disagreed that 5 of the 32 matrix responses were incorrect and that insufficient information was provided for 8 other responses. DARPA also reported that the DARPA Management Support System was formally accredited on September 6, 2002 which included documentation of the certification authority, project manager, and user representative positions. Where appropriate, we revised our discussion of matrix responses as a result of the DARPA comments. However, those revisions did not alter our finding. DARPA nonconcurred with the three report recommendations, stating that the alignment of its information assurance staff positions was correct and appropriate. DARPA also stated that the designated approving authority and certification authority are separate and independent from each other. Further, DARPA stated that security clearance documentation for information systems contract support personnel had always existed and that it would provide this information if requested. The DARPA responses to the recommendations were nonresponsive. DARPA did not address the formal appointment of the three key information assurance staff positions and did not address the organizational alignment of those positions to ensure checks and balances. Additionally, DARPA did not provide supporting documentation that verified the independence of the designated approving authority and the certification authority and the security clearance levels for the information systems contract support personnel with access to the DARPA Management Support System. We request that DARPA reconsider its position on the recommendations and provide additional comments in response to the final report by January 24, 2003. See the Finding section and Appendix C for a discussion of management comments and the Management Comments section for the complete text of the comments.

Table of Contents

Executive Summary	i
Background	1
Objectives	2
Finding	
Defense Advanced Research Projects Agency Management Support System Information Security	3
Appendixes	
A. Scope and Methodology	16
B. Government Information Security Reform Act Collection Matrix Submission	17
C. Summary of DARPA Comments on the Finding and Audit Response	27
D. Report Distribution	37
Management Comments	
Defense Advanced Research Projects Agency	39

Background

Government Information Security Reform. On October 30, 2000, the President signed the Floyd D. Spence National Defense Authorization Act for FY 2001 (Public Law 106-398), which includes title X, subtitle G, the “Government Information Security Reform” (GISR) Act. Subtitle G directs that the Government ensure effective controls for highly networked Federal information resources; management and oversight of information security risks; and a mechanism for improved information system security oversight and assurance for Federal information security programs. The GISR Act directs each Federal agency (DoD for purposes of this report) to annually evaluate its information security program and practices and, as part of the budget process, submit the results of the evaluation to the Office of Management and Budget. The GISR Act covers both unclassified and national information security systems and creates a comparable security management framework for each. The GISR Act also requires that the agency Inspector General or other independent agent evaluate the agency information security program and practices. Also, the GISR Act requires each agency Inspector General or other independent agency to select and test a subset of systems that will confirm the effectiveness of the information security programs.

DoD Responsibilities. The GISR Act directs DoD to annually evaluate its information security program and practices. The DoD uses information technology for thousands of processes that are integral to support and operational functions. Mission-critical, mission-essential, and support-function processes, or applications, reside on computer systems throughout DoD. Applications for the DoD Components include financial accounting; personnel; pay and disbursement; materiel shipping, receiving, and storing; munitions maintenance; and weapon systems-associated applications.

The GISR Act directs that DoD as part of the budget process submit the results of their annual evaluation to the Office of Management and Budget. Office of Management and Budget guidance, memorandum 01-24, “Reporting Instructions for the Government Information Security Reform Act,” June 22, 2001, directs the Secretary of Defense to transmit the FY 2001 annual evaluation of information security program and practices to the Office of Management and Budget by October 1, 2001. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD[C³I]) formed and chaired an Integrated Process Team to develop and finalize the guidance and methodology for DoD reporting of the GISR Act. The Integrated Process Team developed a 32-column spreadsheet--GISR Act collection matrix--to gather data on assessments of the effectiveness of DoD information assurance policies, procedures, and practices. DoD required the FY 2001 GISR Act collection matrix data completion as of August 1, 2001.

Inspector General Responsibilities. Office of Management and Budget issued memorandum 01-08, “Guidance on Implementing the Government Information Security Reform Act,” in January 2001 to provide implementation instructions for Federal agencies in carrying out the GISR Act. Guidance specific to the duties of each Inspector General as an independent evaluator was also included in that memorandum. The Office of Management and Budget guidance states that each

Inspector General or independent evaluator “should perform an annual evaluation of the agency’s security program and practices. This includes testing the effectiveness of security controls for an appropriate subset of agency systems.” Although the GISR Act applies to all Government information systems, Office of Management and Budget acknowledged that agencies could not review all of those systems every year. As a result, the independent evaluation should identify and assess a logical representative sampling of systems that can be used to form the basis of a conclusion regarding the effectiveness of an agency’s overall security program.

DoD Systems. The Office of the Inspector General of the Department of Defense developed a stratified random sample from the population of automated information systems the DoD evaluated and reported for FY 2001 in the “GISR Report FY01: Government Information Security Reform Act, Report of the Department of Defense,” October 2001 (DoD GISR Act Report). DoD selected and reported in the DoD GISR Act Report on a sample of 560 automated information systems from the almost 4,000 systems listed in the DoD Information Technology Registry.¹ The Office of the Inspector General of the Department of Defense stratified random sample included 115 systems from the universe sample of 560 systems that were reported on in the DoD GISR Act Report. The audit agencies for the Military Departments and the Defense Information Systems Agency Inspector General were to evaluate 91 of the 115 information systems in the sample by August 2, 2002. The Office of the Inspector General of the Department of Defense was to evaluate the remaining 24 systems that support DoD agencies and activities. This report discusses the evaluation of 1 of the 24 DoD-level systems, the Defense Advanced Research Projects Agency (DARPA) Management Support System (DMSS).

DoD Information Security Program. DoD Instruction 5200.40, “DoD Information Technology Security Certification and Accreditation Process, (DITSCAP),” December 30, 1997 (hereafter referred to as DITSCAP), provides the procedures for certification and accreditation of information technology to include information systems, networks, and sites in DoD. It also assigns responsibilities for oversight and implementation of the certification and accreditation process. DITSCAP is to be used as guidance throughout the certification and accreditation process. DoD Manual 8510.1-M, “Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual,” July 2000, provides implementation guidance that standardizes the certification and accreditation process throughout DoD.

Objectives

Our overall audit objective was to assess DMSS for implementation of the GISR Act requirements of the Floyd D. Spence National Defense Authorization Act for FY 2001. See Appendix A for a discussion of the audit scope and methodology.

¹The Information Technology Registry was established in response to requirements contained in section 8102(a) of the National Defense Appropriation Act for FY 2001 and section 811(a) of the National Defense Authorization Act for FY 2001. The DoD registry must contain all of the fielded mission-critical and mission-essential systems as well as all the mission-critical and mission-essential systems that are in development.

Defense Advanced Research Projects Agency Management Support System Information Security

Data reported for DMSS in support of the implementation of the GISR Act requirements for FY 2001 were partially inaccurate as of August 1, 2001. DARPA² answered 5 of the 32 GISR Act collection matrix data fields incorrectly. Also, DARPA did not provide documentation that supported 8 of the 32 collection matrix responses. Additionally, the key DARPA information assurance staff positions were not aligned in a way that ensures segregation of duties and the required checks and balances in the DITSCAP for DMSS. Furthermore, DARPA did not formally appoint three of the four key information assurance staff positions required to ensure the appropriate checks and balances during the certification process. Also, the Designated Approving Authority (DAA) was not within the operational chain of command, as DITSCAP requires. Further, DARPA did not provide support that they had verified that the contractors working on the system had proper security clearances. As a result, DMSS may not have adequate information security operational controls that ensure sensitive information is safeguarded.

Mission and System Information

The DARPA mission is to develop imaginative, innovative, and often high-risk research ideas offering a significant technological impact that will go well beyond the normal evolutionary developmental approaches. DARPA pursues the ideas from demonstration of the technical feasibility through development of prototype systems.

System Background. DMSS is a mission-essential³ system that supports DARPA and its various technical offices and support offices. DMSS is a local area network, in Arlington, Virginia, and consists of interconnected systems that provide access to unclassified local area networks and remote workstations. The DMSS network mission is to provide standard automation functions and financial transaction tracking.

Contract Support. In September 2001, DARPA contracted for DMSS hardware, software, and systems support. The contractor provided computers, printers, and other equipment; the software and site licenses that comprise DMSS; and maintenance of the system. Additionally, the contractor would provide the certification and accreditation documentation of the system that DITSCAP required.

²DARPA is the program office for DMSS.

³Mission-essential systems are those systems that are basic and necessary for the accomplishment of an organization's mission.

System Configuration. DMSS is an unclassified network, but all data is considered sensitive. The DMSS network provides financial tracking services, software development for financial applications, security protection services, print services, file services, database services, application services, web services, remote access, Virtual Private Network services, e-mail services, facsimile services, scheduling/calendaring and archive facilities for network servers and user workstations. DMSS uses commercial off-the-shelf software, such as the Microsoft Office Suite products (Access, Excel, Outlook, PowerPoint, and Word).

Data Collection Matrix

DARPA provided the response for the DMSS to ASD(C³I) as of August 1, 2001, and the data reported were partially inaccurate. In response to the GISR Act requirement for each Federal agency to annually evaluate and report on its information security program and practices, ASD(C³I) developed a GISR Act data collection matrix (the matrix) for DoD. The Assistant Secretary developed the matrix as a management tool to track information assurance trends and outcomes. The matrix consisted of a spreadsheet divided into four sections for data. Section titles included identifying information, accreditation information, assessment criteria information, and operations and assessments interest items.

In response to the information requested in the matrix, DARPA was generally required to answer yes, no, or provide a date for action completed. With the exception of a special section that could be used for augmenting comments, no other explanation was required or expected. A discussion of each section of the matrix, the data that DARPA reported in the matrix for DMSS, and our analysis of the data follows. Appendix B contains the DMSS information submitted by DARPA for three of the four sections of the matrix. The section of the matrix that requested identifying information is not presented in Appendix B.

Identifying Information. DARPA was requested to provide the system/network name, acronym, component owner, and information technology classification (mission critical or mission essential) in the identifying information section of the matrix. DARPA responded in the matrix that DMSS was under the component ownership of DARPA and was classified as a mission-critical information technology system. We verified that the identification information in the matrix was incorrectly reported because DMSS was not a mission-critical system but a mission-essential system as stated in the DoD Information Technology Registry.

Accreditation Information. DARPA was requested to provide in the accreditation information section of the matrix the date of accreditation certification, date of interim certification, the accreditation method, and whether formal documentation for certification and accreditation existed.

Accreditation Date. DARPA was requested to provide the date that an accreditation process accredited DMSS. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988, establishes the minimum-security requirements for DoD automated information systems. DITSCAP implements the Directive, assigns responsibility, and prescribes procedures for certification and accreditation. DARPA responded in the matrix that the accreditation is pending. We verified that the DARPA response was appropriate. DARPA did not place a date in the field because DMSS was in the process of applying DITSCAP requirements. The DARPA goal was to accredit the DMSS by September 30, 2002. However, DARPA reported in the management comments to the draft report that DMSS was accredited on September 6, 2002.

Interim Certification Date. DARPA was requested to provide the date that an interim authority to operate was granted. According to the provisions of DITSCAP, interim authority should be based on the establishment of an acceptable level of risk in operating the system. DARPA responded in the matrix that an interim authority to operate was granted to DMSS on July 15, 2001. We verified that the matrix response was essentially correct although the date of the interim authority to operate should have been July 17, 2001. The DAA, Director of the Security and Intelligence Directorate granted interim authority to operate the DMSS. That interim authority was valid for 3 months. Since July 17, 2001, interim authority was renewed three times. The most recent interim authority to operate the DMSS was granted February 22, 2002. Although the interim authority was valid until September 30, 2002, DARPA reported in the management comments to the draft report that DMSS was accredited on September 6, 2002.

Accreditation Method. DARPA was requested to identify whether DMSS was accredited under DITSCAP and, if not under DITSCAP, to describe other accreditation and certification procedures. Several policies govern actions of DMSS program officials, but DITSCAP is the principal governing document for risk assessment and mitigation of DoD information technology systems. DITSCAP establishes the oversight mechanism that ensures identification of appropriate information to certify, accredit, and maintain a program's security. DARPA responded in the matrix that they were using DITSCAP to certify and accredit the DMSS. We verified that the response was incorrect and that the DMSS was following DITSCAP procedures, but DARPA should have responded "no" to the question because as of August 1, 2001, DMSS was not accredited. DARPA reported in the management comments to the draft report that DMSS was accredited on September 6, 2002.

Certification and Accreditation Documentation. DARPA was requested to identify whether formal documentation existed that the Inspector General of the Department of Defense or other entities could use to verify accreditation. DITSCAP requires a System Security Authorization Agreement (SSAA) for each information technology system. The SSAA is a formal and binding document among the system program manager, the DAA, the certifying authority, and the user representative that establishes the level of security required. The SSAA guides the process and documents the results for certification and accreditation as well as implementation of information technology security requirements. DARPA responded in the matrix that they did

not have formal documentation in effect for the DMSS certification and accreditation process. We confirmed that DARPA did not have formal documentation for the DMSS certification and accreditation process as of August 1, 2001. Since then, DARPA has developed an in-process⁴ SSAA.

Assessment Criteria Information. DARPA was requested to confirm that information assurance controls and plans in the assessment criteria information section of the matrix existed. According to the instructions provided for the matrix, ASD(C³I) developed the assessment criteria information section to assess selected systems on the basic program management, controls, and procedures that exist as part of the operation of the system.

Access Controls. DARPA was requested to identify whether access controls were in place. ASD(C³I) defined access controls as controls that limited access of information system resources to authorized users, programs, processes, or other systems. DARPA responded in the matrix that access controls were in place. DARPA did not provide documentation that supported the “yes” response for having access controls in place as of August 1, 2001. As a result, we could not verify the response. However, subsequent to August 2001, we were able to verify that access controls had been implemented. Those access controls that DMSS used included: users were required to identify themselves during system login through the use of a protected mechanism (such as passwords) to authenticate user identity and user accounts; user accounts are locked out and service will be denied for 60 minutes after five unsuccessful login attempts; and passwords expired every 90 days.

Risk Assessment and Management Plan. DARPA was requested to identify whether a risk assessment and management plan had been completed. ASD(C³I) defined risk as the possibility of something adverse happening; risk assessment as the process of analyzing threats and vulnerabilities of an information system and the potential impact of lost information; and risk management as the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. DARPA responded in the matrix that a risk assessment and management plan was completed. We verified that DARPA had a risk assessment and management plan completed as of August 1, 2001. The plan listed procedures for determining minimum information system security requirements.

System Life-Cycle Plan. DARPA was requested to identify whether a system life-cycle plan existed. System life-cycle plan guidance that ASD(C³I) provided with the matrix was that many system life-cycle models exist but most contain five basic phases: initiation, development and acquisition, implementation, operation, and disposal. DARPA responded in the matrix that a DMSS System Life-Cycle Plan was not completed. We confirmed that when DARPA submitted the matrix data as of August 1, 2001, they had not developed a DMSS System

⁴The audit team could not determine the status of many of the documents developed after August 1, 2001. DARPA responded that the documents were operational documents rather than draft or final (approved) documents. As a result, we identified the documents as in-process to indicate that they are not final documents, but are apparently being used by DARPA.

Life-Cycle Plan. However, DARPA has a system life-cycle requirement that called for hardware and software to be replaced when or before either reaches a predetermined age.

System Security Plan. DARPA was requested to identify whether a system security plan was in place. ASD(C³I) defined a system security plan as an overview of the security requirements of a system, a description of the controls in place or the controls planned for meeting those requirements, and delineation of responsibilities and expected behavior of the individuals who access the system. DARPA responded in the matrix that a DMSS System Security Plan was not completed. We confirmed that when DARPA submitted the matrix data as of August 1, 2001, they had not developed a DMSS System Security Plan. However, since that time, DARPA developed a DMSS System Security Plan. The plan serves as a security policy document and provides security services for protection of information systems. Further, the plan identifies security mechanisms in place on the DMSS and was expanded to include security policies and procedures necessary to support the changing environment.

Personnel Security Measures. DARPA was requested to identify whether proper personnel security measures were in place. ASD(C³I) defined personnel security measures as a broad range of security issues related to how human users, designers, implementers, and managers of software and hardware interact with computers, and the access and authorities needed to do their jobs. DARPA responded in the matrix that DMSS had personnel security measures in place. DARPA did not provide documentation that supported the “yes” response for having personnel security measures in place as of August 1, 2001. As a result, we could not verify the response. Subsequent to August 2001, we were able to verify that personnel security measures had been implemented. DMSS had segregation of duties, with varying levels of control: the individual must have at least a SECRET clearance and been granted access to the system based on a “need to know;” the individual received appropriate training in system capabilities and security procedures; and foreign nationals who possess a SECRET clearance may be granted access to the DMSS only after written approval of the DAA and only to the unclassified network. DMSS password protection procedures required that passwords change every 90 days and accounts are terminated either when the user is no longer employed or for misuse.

Physical Security Controls. DARPA was requested to identify whether physical security controls were in place. ASD(C³I) defined physical security and environment security as the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. DARPA responded in the matrix that DMSS had physical security controls in place. We verified that physical security controls were in place as of August 1, 2001. An electronic card access system controlled primary access to the DARPA office suites on a 24-hour basis. In addition, closed-circuit television cameras provided coverage of the exterior perimeter doors and the sidewalks immediately adjacent to the building. Unarmed guard patrols were conducted around the building perimeter and the office spaces after hours. Since August 1, 2001, DARPA implemented additional physical security controls. They include

an Arlington County policy officer stationed outside the DARPA main building 24 hours a day and the revocation of on-the-street parking adjacent to the DARPA building.

Administrative Controls. DARPA was requested to identify whether administrative controls were in place. ASD(C³I) did not define administrative controls but suggested that administrative controls included the presence of a help desk and audit trail. Administrative controls are designed to promote operational efficiency and adherence to system policies and procedures. DARPA responded in the matrix that DMSS had administrative controls in place. However, DARPA did not provide documentation that supported the “yes” response as of August 1, 2001. As of August 1, 2001, we verified that DARPA had a help desk, but we could not verify that DARPA had established audit trails. However, DARPA provided documentation indicating that audit trails had been established subsequent to August 1, 2001.

Contingency Plans. DARPA was requested to identify whether contingency plans were in place and, if so, when the last time was that a contingency drill, data loss drill, or power loss drill occurred. ASD(C³I) defined contingency planning as involving more than simply planning for a move offsite after a disaster destroys a facility. Contingency planning was to also include how to keep an organization’s critical functions operational in the event of disruptions, both large and small. DARPA responded in the matrix that DMSS had a contingency plan in place. We verified that DARPA had a contingency plan for 2000; however, DARPA should have responded “no” because the “yes” response was based on the 2000 Contingency Plan. That plan discussed two DARPA mission-essential systems: the main DARPA building and the financial information system. The plan does not mention DMSS or similar local area network system that predated DMSS.

DoD Directive 5200.28 requires periodic testing of contingency plans for mission-critical systems and encourages contingency plans for all systems. DARPA responded in the matrix that DMSS was last exercised December 30, 1999. We verified that the contingency plan was exercised in the December 1999 time frame. However, DARPA should not have answered with a date because the exercise was based on a year 2000 contingency plan. Furthermore, the 2000 Contingency Plan exercise focused only on interruptions for 2000.

Since August 2001, DARPA developed an in-process Business Resumption Plan that provides the procedures necessary to recover critical DARPA business functions in the event of a disaster.

Hardware and System Software Maintenance Plans. DARPA was requested to identify whether hardware and software maintenance plans were in place. ASD(C³I) defined hardware and software maintenance plans as controls used for monitoring the installation of, and update to, hardware and software to ensure that the system functions as expected and that a historical record of changes is maintained. DARPA responded in the matrix that DMSS had hardware and system software maintenance plans in place. However, DARPA did not provide documentation that supported the “yes” response as of August 1, 2001. As a result, we could not verify the response.

Subsequent to August 2001, we were able to verify that DARPA has a configuration management plan, used to manage configuration of hardware and software. In addition, DARPA chartered the DARPA Configuration Control Board to control the DMSS configuration. The board was to establish procedures for controlling changes in configuration items.

Data Integrity Process. DARPA was requested to identify whether data integrity processes were in place. ASD(C³I) defined data integrity processes as controls used to protect data from accidental or malicious alteration or destruction and used to provide assurance for users that the information met expectations about its quality and integrity. DARPA responded in the matrix that DMSS had data integrity processes in place. DARPA did not provide documentation that supported the “yes” response as of August 1, 2001. As a result, we could not verify the response. However, DARPA has subsequently developed in-process documents indicating that DMSS currently has a data integrity process in place. Virus scans and communication encryption software protected the DMSS.

Security Incident Response Plan. DARPA was requested to identify whether a security incident response plan was in place. ASD(C³I) defined a security incident response plan as a formal description and evaluation of risks to an information system, and a process that identified and applied countermeasures commensurate with the value of the assets protected based on a risk assessment. An incident response plan should have help capability when an adverse event in a computer system or network causes a failure of a security mechanism or when an attempted breach of those mechanisms occurs. DARPA responded in the matrix that DMSS had a security incident response plan in place. DARPA did not provide documentation that supported the “yes” response as of August 1, 2001. As a result, we could not verify the response. Further, DARPA did not provide documentation to indicate the current status of the existence of a security incident response plan.

Operations and Assessments Interest Items. DARPA was requested to identify specific operational assessment mechanisms that existed as part of the operation of the system and to provide general comments that would augment reporting efforts on basic program management, controls, and procedures. ASD(C³I) did not provide definitions for reporting elements contained in the operations and assessments interest items section of the matrix. Information contained in that section included network protections, vulnerabilities, and assessments.

Network Protections. ASD(C³I) requested data on the network security functions of intrusion detection software and firewalls from DARPA.

Intrusion Detection Software. DARPA was requested to identify whether intrusion detection software protected the DMSS. Intrusion detection software inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

Firewalls. DARPA was requested to identify whether boundary protections, such as firewalls, for DMSS were present. A firewall is a boundary protection system that limits access between networks to prevent intrusions from outside the network. A firewall stops external intrusions, but does not detect an attack from inside the network. DARPA responded in the matrix that intrusion detection software protected DMSS and that DMSS had boundary protection in place. DARPA did not provide documentation that supported the “yes” responses as of August 1, 2001. As a result, we could not verify the responses. However, DARPA developed in-process documents since August 2001 that confirm intrusion detection software and boundary protection (firewalls) protect DMSS.

Vulnerabilities. ASD(C³I) requested DMSS information from DARPA concerning the red and blue team assessment, connections, information assurance vulnerability alert process, and the vulnerability analysis and assistance program.

Red and Blue Team Assessment. DARPA was requested to identify the date for the most recent red and blue team assessment. According to a dictionary and reference guide used by the GISR Act Integrated Process Team, a red team is a simulated opposing force that uses active and passive actions, as well as technical and non-technical capabilities, to expose and exploit information operation vulnerabilities of a blue team (a simulated friendly force). DARPA responded in the matrix that DMSS had a blue team assessment performed on February 8, 2000. The DARPA response was incorrect. DARPA should not have answered with a date because, according to the DARPA comments on the draft report, an independent vulnerability assessment was performed on February 8, 2000, not a blue team assessment. The blue team assessment was performed in 2002.

Connections. DARPA was requested to identify whether DMSS had a connection approval to connect to a larger backbone network. Connections are system interfaces to other information systems used for transmitting or receiving data. DARPA responded in the matrix that the DMSS interface connections were approved. The DARPA response was correct. DARPA stated it had a waiver, granted by ASD(C³I), to connect to the Internet.

Information Assurance Vulnerability Alert. DARPA was requested to identify whether DMSS was fully information assurance vulnerability alert compliant in both acknowledging and adhering to information assurance vulnerability alerts. An information assurance vulnerability alert is a process that incorporates identification and evaluation of new vulnerabilities, disseminates technical responses, and tracks compliance within DoD. Alerts are generated when a critical vulnerability that poses an immediate threat to DoD exists. DARPA responded in the matrix that DMSS was fully information assurance vulnerability alert compliant. We confirmed that the DARPA response was appropriate as of August 1, 2001; DMSS was information assurance vulnerability alert compliant.

Vulnerability Analysis and Assistance Program. DARPA was requested to identify whether DMSS had a vulnerability analysis and assistance program assessment. According to a dictionary and reference guide used by the GISR Act Integrated Process Team, a vulnerability analysis and assistance program was a survey of the Non-Secure Internet Protocol Router Network, the

SECRET Internet Protocol Router Network, and Joint Worldwide Intelligence Communications System networks for common computer security vulnerabilities. DARPA provided an “NA” response in the matrix. We confirmed that the DARPA response was appropriate as of August 1, 2001, and no vulnerability analysis and assistance program assessment had been performed.

Assessments. DARPA was requested to identify the dates for the most recent:

- Joint Staff integrated vulnerability assessment,
- system requirements reviews,
- balance survivability assessment, and
- integrated vulnerability assessment.

DARPA responded in the matrix that none of these assessments had been performed. We confirmed that the DARPA responses were correct as of August 1, 2001, because the reporting elements in the section were specific assessments and technical controls that not all systems were required to perform.

Site Operational Review

We performed a site operational review at DARPA headquarters, Arlington, Virginia, to verify that information security operational controls were in place for DMSS. As of June 2002, DARPA had access and physical security controls in place. Access controls included password protection, intrusion detection software, and information assurance vulnerability alerts. Physical security controls included electronic card access to office suites, color-coded identification badges, and 24-hour security the Arlington County Police Department provided. However, the key DARPA information assurance staff positions were not aligned in a way that ensures segregation of duties and the required checks and balances in the DITSCAP for DMSS. Furthermore, DARPA did not formally appoint three of the four key information assurance staff positions required to ensure checks and balances during the certification process. Also, the DAA was not within the operational chain of command, as the DITSCAP requires. Further, DARPA did not provide support that they had verified that the contractors working on the system had proper security clearances. As a result, DMSS may not have adequate information security operational controls that ensure sensitive information is safeguarded.

DITSCAP Guidance

DITSCAP states that the key roles in the certification and accreditation process are those functions that the systems program manager, the DAA, the certification authority, and the user representative perform. The DITSCAP also states that those four roles--program manager, DAA, certification authority, and user representative--each represent different views and as such provide the checks and balances that ensure the minimum security requirements are met. Further, DITSCAP requires that the four key information assurance staff positions be appointed during the first phase of the certification and accreditation process.

DITSCAP also discusses the roles and responsibilities of each of the four key information assurance positions during all phases of the certification and accreditation process. The program manager represents the interests of the system acquisition or maintenance organization with engineering, schedule, and funding responsibility. The DAA represents the interest of the organization mission needs, controls the operating environment, and defines the system level security requirements. In addition, the DAA should be a senior member of the operational chain of command where the system is operating. The certification authority provides the technical expertise to conduct the certification by testing the security controls. The interests of the users are vested in the user representative. The user representative is concerned with systems availability, access, integrity, functionality, and performance.

Results of Review

The key DARPA information assurance staff positions were not aligned in a way that would ensure segregation of duties necessary for the checks and balances to ensure minimum security requirements for DMSS. A description of the duties for each of the key information assurance staff positions was included in "DARPA Management Support System (DMSS) Information System Security Plan," November 15, 2001 (System Security Plan). According to the list in the System Security Plan, both the DAA and certification authority positions were listed as duties the Director of the Security and Intelligence Directorate performed. Assigning both of those key positions to the same management official does not provide adequate checks and balances of key management oversight functions. The DAA oversight management function is to define the system level security requirement and the certifying authority is to test the security controls for compliance with security requirements. The program manager was listed as the DARPA hardware and software support contractor. The user representative was listed as the Director of the Information Resources Directorate.

Additionally, DARPA did not formally appoint three of the four key information assurance staff positions. Of the four key information assurance positions--program manager, DAA, certification authority, and user representative--the DAA was the only official formally appointed as of June 2002. The one formally appointed key information assurance position, the DAA for DARPA automated information systems, was the Director of the Security and Intelligence Directorate rather than an official from the operational chain of command such as an official from the DARPA Information Resources Directorate. DARPA officials stated that the certification authority, user representative, and program manager would not be formally appointed until DMSS was accredited. DARPA planned to have DMSS accredited by September 30, 2002. DARPA reported in the management comments to the draft report that DMSS was accredited on September 6, 2002 which included documentation of the certification authority, project manager, and user representative positions.

On-site contractor personnel provided DMSS information security functions as well as software and hardware support. The System Security Plan requires that all personnel having access to DMSS have a SECRET security clearance or higher.

DARPA did not provide us with any supporting documentation that they had verified contractor personnel security clearances prior to granting access to DMSS.

Management Comments on the Finding and Audit Response

DARPA Comments on Physical Security Controls. DARPA stated the report implied the only physical security control in place as of August 1, 2001, was the electronic card access system.

Audit Response. We revised the discussion to reflect that additional physical security controls were in place.

DARPA Comments on Red and Blue Team Assessment. DARPA stated that the draft report was incorrect in stating that DARPA had a blue team assessment in February 2000; the blue team assessment was documented in 2002. The document cited in the draft report was not a blue team assessment but an independent vulnerability assessment.

Audit Response. We revised the discussion to state that the positive matrix response (February 2000 date) submitted by DARPA for blue team assessment was incorrect.

DARPA Comments on Connection Approval. DARPA stated that the discussion section on Connections was incorrect. DARPA stated that DMSS is connected to a larger backbone network (the Internet). That connection is based on a waiver granted by ASD(C³I).

Audit Response. We revised the discussion to state that the DARPA matrix answer was correct.

A summary of DARPA comments on the finding and our audit response is in Appendix C. The complete text of DARPA comments is in the Management Comments section of this report.

Recommendations, Management Comments, and Audit Response

1. We recommend that the Director, Defense Advanced Research Projects Agency formally appoint a program manager, certification authority, and user representative for the Defense Advanced Research Projects Agency Management Support System and require appointments that are organizationally aligned in a way that will provide checks and balances the DoD Information Technology Security Certification and Accreditation Process requires.

DARPA Comments. DARPA nonconcurred, stating that alignment of information assurance staff positions is correct and appropriate for DARPA. Also,

DARPA stated that it follows DITSCAP requirements to achieve the checks and balances appropriate for DARPA. DITSCAP places the decisions involved in those assignments at the Component level. Further, DARPA stated that the three key positions were documented at the formal accreditation signing in September 2002.

Audit Response. DARPA comments were nonresponsive. DITSCAP requires that the key roles (DAA, program manager, certification authority, and user representative) must be appointed during the first phase of the certification and accreditation process. Additionally, DITSCAP states that “the DAA, the CA [certification authority], the program manager, and the user representative each represent different views and as such provide the checks and balances to ensure the minimum-security requirements are met.” As of the end of the audit period, August 2002, DARPA had not formally appointed three of the four key information assurance staff positions. Only the DAA had been appointed and DARPA officials stated that the certification authority, user representative, and program manager would not be formally appointed until DMSS was certified. DARPA comments indicate that the appointments were documented at the formal accreditation. We request the supporting documentation. Further, according to the list in the DARPA System Security Plan (an operational document dated November 15, 2001, 3 months after DARPA submitted the GISR Act matrix data) both the DAA and certification authority positions were listed as duties the Director of the Security and Intelligence Directorate performed. Assigning both of those key positions to the same management official does not provide adequate checks and balances of key management oversight functions. We request that DARPA reconsider its position on the recommendation and provide additional comments and documents in response to the final report.

2. We recommend that the Director, Defense Advanced Research Projects Agency verify that the certification authority and designated approving authority are separate and independent from each other.

DARPA Comments. DARPA nonconcurred, stating that those positions are and have been separate and independent since the initiation of the DITSCAP work. Further, DARPA stated that the Chief Information Officer “supervises both positions to ensure independent work, advice, and visibility and resolution of any conflict.”

Audit Response. DARPA comments were nonresponsive. DARPA did not provide supporting documentation that verified the independence of the certification authority and the DAA given that both the DAA and certification authority positions were listed as duties the Director of the Security and Intelligence Directorate performed. We request that DARPA provide documentation that demonstrates that the certification authority and DAA are separate and independent from each other in its response to the final report.

3. We recommend that the Director, Defense Advanced Research Projects Agency properly document the security clearance levels for all of the information systems contract support personnel that have access to the Defense Advanced Research Projects Agency Management Support System.

DARPA Comments. DARPA nonconcurred, stating that the documentation has always existed, but was not requested.

Audit Response. DARPA comments were nonresponsive. We requested but DARPA did not provide documentation that it verified the security clearances of contractor support personnel before granting access to DMSS because security clearances were not specifically addressed on the GISR Act matrix. We request that DARPA provide the supporting documentation to demonstrate that contractor personnel security clearances are verified before they gain access to DMSS in response to the final report.

Appendix A. Scope and Methodology

We verified and validated the DMSS data supporting the DoD GISR Act Report. We also performed a DMSS site operational review at DARPA to validate operational controls. To accomplish the audit objective, we:

- reviewed Public Law 106-398, Office of Management and Budget guidance, and the DoD regulations and guidance related to the GISR Act;
- interviewed DMSS personnel in DARPA responsible for the GISR Act matrix submission;
- verified the information reported on the GISR Act data collection matrix. Our verification consisted of reviewing the documentation that supported the answers DARPA provided on the GISR Act collection matrix as of August 1, 2001; and
- reviewed site operations that documented the presence of operational controls at DARPA.

We performed this audit from April through August 2002 in accordance with generally accepted government auditing standards. We did not review the management control program because DoD recognized information assurance programs as a material weakness in its FY 2000 Statement of Assurance, which was the most recent, signed Statement of Assurance.

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in DoD. This report provides coverage of the Information Security high-risk area.

Prior Coverage

No prior coverage has been conducted on DMSS during the last 5 years.

Appendix B. Government Information Security Reform Act Collection Matrix Submission

We evaluated the DMSS GISR Act collection matrix that DARPA submitted as of August 1, 2001, to ASD(C³I). The following is a summary on the data ASD(C³I) requested, the response from DARPA, and our audit analysis of the response for 27 of 32¹ fields on the data collection matrix. A list of acronyms is at the end of this appendix.

Accreditation Information		
Data Requested	DARPA Response ²	Audit Results
Accredited? (Date)	Pending	DMSS was not accredited. DARPA stated in comments to the draft report that DMSS was accredited on September 6, 2002.
Interim authority to operate? (Date)	July 15, 2001	The matrix response should have been July 17, 2001, the date of the interim authority to operate. The DAA, Director of Security and Intelligence Directorate, granted interim authority to operate the DMSS for 3 months. The interim authority was renewed three times since July 17, 2001. The most recent interim authority to operate the DMSS was granted February 22, 2002, and valid until September 30, 2002. However, DARPA reported in the management comments to the draft report that DMSS was accredited on September 6, 2002.
Accreditation under DITSCAP?	Yes	The DARPA response was incorrect. DARPA should have responded “no” because DMSS was not accredited as of August 1, 2001. DARPA was following DITSCAP to certify and accredit DMSS and stated in comments to the draft report that DMSS was accredited on September 6, 2002.

¹We did not include in the matrix five administrative information data fields that identified the system. One administrative information data field was answered incorrectly by DARPA. (DMSS was not a mission-critical system but a mission-essential system as stated in the DoD Information Technology Registry.) Of the 27 DARPA responses in this matrix, 4 were incorrect and 8 could not be verified because DARPA did not provide sufficient documentation.

²Some questions requested a date only. If a date was provided, the implied answer was yes.

Accreditation Information (cont'd)		
Data Requested	DARPA Response²	Audit Results
Not DITSCAP, describe other.	Blank	DMSS was not accredited prior to the current effort to accredit under DITSCAP.
Formal documentation in effect? (SSAA or other certification and accreditation documentation)	No	No formal SSAA had been developed for DMSS. Since August 2001, DARPA developed an in-process SSAA.

²Some questions requested a date only. If a date was provided, the implied answer was yes.

Assessment Criteria Information		
Data Requested	DARPA Response ²	Audit Results
Access controls in place?	Yes	<p>DARPA did not provide documentation that supported the “yes” response for having access controls in place as of August 1, 2001. As a result, we could not verify the response.</p> <p>However, DARPA had developed in-process documents since August 2001 that confirmed the DMSS used passwords and user accounts.</p> <ul style="list-style-type: none"> – User accounts were user’s first name initial and last name. – Valid passwords were at least nine alphanumeric characters, with both upper and lower case, and had at least one special character. – After five unsuccessful login attempts, the DMSS user account was locked out and service was denied for 60 minutes. If access was needed sooner, the DARPA Help Desk unlocked the account. – Passwords expired every 90 days.
Risk Assessment and Management Plan completed?	Yes	<p>DARPA had a risk assessment and management plan completed as of August 1, 2001.</p> <p>The plan listed procedures for determining minimum information system security requirements.</p>
System Life-Cycle Plan exists?	No	<p>DARPA did not have a DMSS System Life-Cycle Plan as of August 1, 2001.</p> <p>However, DARPA has a system life-cycle requirement that called for hardware and software to be replaced when or before either reaches a predetermined age.</p>

²Some questions requested a date only. If a date was provided, the implied answer was yes.

Assessment Criteria Information (cont'd)		
Data Requested	DARPA Response ²	Audit Results
System Security Plan in place?	No	<p>DARPA did not have a DMSS System Security Plan as of August 1, 2001.</p> <p>However, since that time, DARPA developed a DMSS System Security Plan. The plan serves as a security policy document and provides security services for protection of information systems. Further, the plan identifies security mechanisms in place on the DMSS and was expanded to include security policies and procedures necessary to support the changing environment.</p>
Proper personnel security measures in place? (includes assignment of duties and segregation of duties)	Yes	<p>DARPA did not provide documentation that supported the “yes” response for having personnel security controls in place as of August 1, 2001. As a result, we could not verify the response. However, DARPA developed in-process documents since August 2001 that confirmed the DMSS had personnel security controls in place. DMSS had segregation of duties, with varying levels of access and control.</p> <ul style="list-style-type: none"> – The individual must have at least a SECRET clearance and been granted access based on a “need to know.” – The individual had received appropriate training in system capabilities and security procedures. – Foreign nationals who possessed a SECRET clearance may be granted access to the DMSS only after written approval of the DAA and only to the unclassified network. <p>Passwords were changed every 90 days. Accounts were terminated when the user was no longer actively employed or for misuse.</p>

²Some questions requested a date only. If a date was provided, the implied answer was yes.

Assessment Criteria Information (cont'd)		
Data Requested	DARPA Response ²	Audit Results
Physical security controls in place?	Yes	<p>As of August 1, 2001, we verified that a 24-hour electronic card access system and other after-business-hours controls, such as closed-circuit television and unarmed guards, were providing the primary access controls for the DARPA office suites.</p> <p>Since August 2001, DARPA implemented additional physical security controls, to include armed guards, and an Arlington County police officer was stationed outside of the DARPA main building 24 hours a day.</p>

²Some questions requested a date only. If a date was provided, the implied answer was yes.

Assessment Criteria Information (cont'd)		
Data Requested	DARPA Response ²	Audit Results
Administrative controls in place? (includes help desk and audit trail)	Yes	DARPA did not provide documentation that supported the "yes" answer as of August 1, 2001. As of August 1, 2001, we verified that DARPA had a help desk, but we could not verify that DARPA had established audit trails. However, DARPA provided documentation indicating that audit trails have been established subsequent to August 1, 2001.
Contingency Plans in place?	Yes	<p>The DARPA response was incorrect. DARPA should have responded "no" because the "yes" response was based on a contingency plan for 2000. That plan addressed only 2000 activities and did not address contingency operations in a broader context.</p> <p>Since August 2001, DARPA developed an in-process Business Resumption Plan that provided the procedures necessary to recover critical DARPA business functions in the event of a disaster.</p>
Date contingency plans last exercised?	December 30, 1999	The DARPA response was incorrect. The DARPA 2000 Contingency Plan was exercised in the December 1999 time frame but was performed for 2000 concerns and not applicable to current conditions.
Hardware and system software maintenance plans in place? (includes version control testing)	Yes	<p>DARPA did not provide documentation that supported the "yes" response as of August 1, 2001. As a result, we could not verify the response.</p> <p>Since August 2001, DARPA developed a configuration management plan, used to manage configuration of DMSS hardware and software. In addition, DARPA chartered the DARPA Configuration Control Board to control the DMSS configuration. The board was to establish procedures for controlling changes in configuration items.</p>

²Some questions requested a date only. If a date was provided, the implied answer was yes.

Assessment Criteria Information (cont'd)		
Data Requested	DARPA Response²	Audit Results
Data integrity process in place? (includes virus scans, system performance monitoring)	Yes	<p>DARPA did not provide documentation that supported the “yes” response as of August 1, 2001. As a result, we could not verify the response.</p> <p>DARPA subsequently developed in-process documents that confirmed the DMSS has a data integrity process in place.</p> <p>Virus scans and communication encryption software protected DMSS.</p>
Security incident response plan in place?	Yes	<p>DARPA did not provide documentation that supported the “yes” response as of August 1, 2001. As a result, we could not verify the response.</p> <p>DARPA did not provide documentation that indicated the current status.</p>

²Some questions requested a date only. If a date was provided, the implied answer was yes.

Operations and Assessments Interest Items

Data Requested	DARPA Response²	Audit Results
Protected by IDS [Intrusion Detection Software]?	Yes	DARPA did not provide documentation that supported the “yes” response as of August 1, 2001. As a result, we could not verify the response. However, DARPA developed in-process documents since August 2001 that confirmed IDS protected DMSS.
Boundary protection in place? (For example, firewall)	Yes	DARPA did not provide documentation that supported the “yes” response as of August 1, 2001. As a result, we could not verify the response. DARPA developed in-process documents since August 2001 that confirmed boundary protection (firewalls) protect DMSS. Unsuccessful login attempts were tracked.
Red and blue team assessment? (Date)	February 8, 2000	The DARPA response was incorrect. DARPA should not have answered with a date because, according to the DARPA comments on the draft report, an independent vulnerability assessment was performed on February 8, 2000, not a blue team assessment. The blue team assessment was performed in 2002.
Connection approved?	Yes	The DARPA response was correct. DARPA stated that they had a waiver from ASD(C ³ I) to connect to the Internet.
IAVA [Information Assurance Vulnerability Alert] compliant?	Yes	We confirmed that the DARPA response was appropriate as of August 1, 2001, because DMSS was information assurance vulnerability alert compliant.

²Some questions requested a date only. If a date was provided, the implied answer was yes.

Operations and Assessments Interest Items (cont'd)		
Data Requested	DARPA Response²	Audit Results
VAAP [Vulnerability Analysis and Assistance Program] assessment complete? (Date)	NA	VAAP was not required and not applicable to DMSS.
Joint Staff integrated vulnerability assessments complete? (Date)	No	No Joint Staff integrated vulnerability assessments were completed for DMSS.
System requirements reviews complete? (Date)	No	No system requirements reviews were completed for DMSS.
Balance survivability assessment complete? (Date)	No	No balance survivability assessment was completed for DMSS.
Integrated vulnerability assessment complete? (Date)	No	No integrated vulnerability assessment was completed for DMSS.

²Some questions requested a date only. If a date was provided, the implied answer was yes.

Applicable Acronyms

ASD(C ³ I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
DAA	Designated Approving Authority
DARPA	Defense Advanced Research Projects Agency
DITSCAP	Defense Information Technology Security Certification and Accreditation Process
DMSS	Defense Advanced Research Projects Agency Management Support System
GISR	Government Information Security Reform
IAVA	Information Assurance Vulnerability Alert
IDS	Intrusion Detection Software
SSAA	System Security Authorization Agreement
VAAP	Vulnerability Analysis and Assistance Program

Appendix C. Summary of DARPA Comments on the Finding and Audit Response

The following is a summary of DARPA comments on the finding and our audit response to those comments.

Mission and System Information

DARPA Comments on Contract Support. DARPA nonconcurred with the report statement, “In September 2001, DARPA contracted for DMSS hardware, software, and systems support.” DARPA stated, “The DMSS is a legacy system and has existed since the early 1980s. It and other Information Technology (IT) assets were transferred to the extant contractor under a modified managed services contract awarded in April 2001.”

Audit Response. The modified managed services contract was awarded in April 2001 by the Department of Transportation. However, the delivery order on the Department of Transportation contract for DARPA managed services requirements was not issued until September 2001.

Data Collection Matrix

DARPA Comments on Accreditation Method. DARPA nonconcurred with our conclusion that its matrix response on DMSS accreditation under DITSCAP was incorrect. DARPA stated:

The matrix question is “Accreditation under DITSCAP?” This question asks if DITSCAP is the framework under which accreditation is developed, not whether accreditation has been completed (which is asked separately above it). DARPA is correct to respond “Yes” in that DARPA was using DITSCAP as the basis for all accreditation and certification work.

Audit Response. The co-chairman of the GISR Act Integrated Process Team stated that it was the direction and intent of the Office of the Secretary of Defense that activities should respond “no” to items where there was no formal/approved documentation. DARPA did not have formal/approved documentation on DITSCAP accreditation for DMSS as of August 1, 2001, the matrix submission date. Therefore, its matrix response should have been “no” because DMSS was not accredited under DITSCAP as of August 1, 2001.

DARPA Comments on Certification and Accreditation Documentation. DARPA nonconcurred with the term “in-process,” which was used throughout the report. DARPA stated:

The DoDIG term “in-process” is misleading and does not convey the true state of the accreditation documents given to the DoDIG. Those documents were complete and reviewed by senior management at the time they were written. Because the DMSS is a dynamic system, with frequent (often weekly) changes, the supporting documents are under constant revision. They could not, by definition, be “approved” until formal accreditation.

Audit Response. We believe “in-process” is an appropriate term to describe documents “under constant revision,” as stated by DARPA.

DARPA Comments on Access Controls. DARPA nonconcurred with our report statement, “DARPA did not provide documentation that supported the ‘yes’ response for having access controls in place as of August 1, 2001.” DARPA stated:

The DoDIG requested specific documentation in writing. DARPA provided that documentation and did not receive any response stating such documentation was insufficient for their needs. The documentation provided to the DoDIG was DITSCAP documentation dated after August 1, 2001, which details the physical, technical, and administrative controls in place to protect the DMSS.

Audit Response. We requested access control documentation as of August 1, 2001, in order to verify the DMSS data provided in the matrix. The access control document DARPA provided us was dated December 10, 2001, which is after the cut-off date.

DARPA Comments on System Life-Cycle Plan. DARPA nonconcurred with the draft report statement, “We confirmed that when DARPA submitted the matrix data as of August 1, 2001, they had not developed a DMSS System Life-Cycle Plan. However, since that time, DARPA has a system life-cycle requirement that called for hardware and software to be replaced when or before either reaches 24 months of age.” DARPA stated:

DARPA has always had a life-cycle requirement for refreshment of DMSS components. As of April 2001, the effective date of the latest contract for DMSS support, this requirement was 24 months. Prior to that, it was 36 months.

Audit Response. We modified the report, which now reads: “However, DARPA has a system life-cycle requirement that called for hardware and software to be replaced when or before either reaches a predetermined age.”

DARPA Comments on Personnel Security Measures. DARPA nonconcurred with the report statement that it did not provide documentation that supported the “yes” response for having personnel security measures in place as of August 1, 2001. DARPA stated:

This is an incorrect statement. The DoDIG requested specific documentation in writing. . . . The documentation provided to the

DoDIG was DITSCAP documentation dated after August 1, 2001, which details the controls related to personnel security that were in place to protect the DMSS.

Audit Response. We requested documentation that supported the “yes” response regarding the presence of personnel security measures as of the date that DARPA submitted the DMSS matrix data, August 1, 2001. The personnel security documents DARPA provided were dated November 2001.

DARPA Comments on Physical Security Controls. DARPA stated that the section on Physical Security Controls was misleading, adding:

The wording implies that on August 1, 2001, DARPA had only its electronic card access system in place as a physical security control. It implies that the other controls were added after August 1, 2001. All security measures mentioned here, with the exceptions of armed (vs. unarmed) guards and an on-station Arlington County police officer, have been in place at DARPA for many years.

Audit Response. We revised the Physical Security Controls section to reflect DARPA concerns.

DARPA Comments on Administrative Controls. DARPA stated that the report section on Administrative Controls contained incorrect statements, specifically noting:

The DoDIG requested specific documentation in writing. . . . The documentation provided to the DoDIG was DITSCAP documentation dated after August 1, 2001, which indicates that administrative controls were in place. Similar controls have been in place since the initial implementation of the DMSS in the early 1980s.

Audit Response. We requested administrative control documentation as of August 2001 to verify the DMSS data provided in the matrix. As stated in the DARPA response, the administrative control documentation DARPA provided us was dated after August 1, 2001.

DARPA Comments on Contingency Plans. DARPA provided four separate comments on the contingency plan portion of the report.

- DARPA stated that the report statement indicating that DARPA should have responded “no” because the “yes” response was based on the 2000 Contingency Plan was incorrect. DARPA stated:

There is no basis in fact for saying that a Y2K [year 2000] contingency plan is not appropriate for future use. . . . That documentation, with its detailed procedures for responding to a wide range of disruptions, including total system replacement, was a highly useful contingency plan on August 1, 2001.

-
- DARPA stated that the report was incorrect in stating that the contingency plan discussed two DARPA mission-essential systems: the main DARPA building and the financial information system. DARPA stated:

There is only one DARPA system, which is the mission-essential DMSS, so named in the DoD Y2K Data Base, which preceded the DoD IT Registry. The voluminous plan discusses nothing but the DMSS, DARPA's single local area network, including all attachments and peripherals.

- DARPA stated that the report was incorrect with respect to the statement that DARPA should not have provided a date because the exercise was based on a year 2000 contingency plan. DARPA stated:

[T]here is no basis for categorically stating the plan should not have been used for an exercise just because it was developed for Y2K concerns. In fact, it is as good and appropriate a plan as could have been used at the time, with no additional costs incurred.

- DARPA also nonconcurred with the statement in the report, "Furthermore, the 2000 Contingency Plan exercise focused only on interruptions for 2000."

This is an incorrect statement. . . . [T]he 2000 Contingency Plan provides detailed procedures covering the widest possible range and degree of disruptions, whether those disruptions might be caused by utility failures, fire, flood, malicious intent, or other problems. The DoDIG based its report on less than 1 percent of the Y2K documentation.

Audit Response. DARPA provided a document titled "DARPA Y2K Contingency Planning" to the audit team in response to our request for a contingency plan as of August 1, 2001. The document stated that "DARPA has two 'mission-essential' systems, the main DARPA building and the financial information system." The document did not mention DMSS or a similar legacy system that predated DMSS. DARPA did not indicate that this was a partial or incomplete document. If documents existed, they were not provided. DARPA responded in the matrix that DMSS was last exercised December 30, 1999. We verified that the contingency plan was exercised in the December 1999 time frame. However, DARPA should not have answered with a date because the exercise was based on a year 2000 contingency plan. Furthermore, the 2000 Contingency Plan exercise focused only on interruptions for 2000.

DARPA Comments on Hardware and Software Maintenance Plans. DARPA stated that the report section on Hardware and System Software Maintenance Plans was incorrect in stating that the "yes" answer was incorrect. DARPA stated it had hardware and software maintenance plans in place prior to August 1, 2001.

Audit Response. We requested hardware and software maintenance plan documentation as of August 2001, to verify the DMSS data provided in the matrix. The hardware and software maintenance plan documentation DARPA provided was dated after August 1, 2001.

DARPA Comments on Data Integrity Process. DARPA stated that the report section on Data Integrity Process was incorrect, adding:

The documentation provided to the DoDIG was DITSCAP documentation dated after August 1, 2001, which details an in-place data integrity process that protects DMSS data Similar procedures have been in place since the initial implementation of the DMSS in the early 1980s.

Audit Response. We requested data integrity process documentation as of August 2001 to verify the DMSS data provided in the matrix. The data integrity process documentation DARPA provided was dated after August 1, 2001.

DARPA Comments on Security Incident Response Plan. DARPA stated that the statement about documentation in the Security Incident Response Plan section was incorrect, adding:

The DoDIG requested specific documentation in writing. . . . The documentation provided to the DoDIG details our security incident response plan that is in place to protect the DMSS from adverse events that could cause a failure of security mechanisms or when an attempted breach of these mechanisms occurs.

Audit Response. We requested security incident response plan documentation as of August 2001 to verify the DMSS data provided in the matrix. We did not receive any Security Incident Response Plan documentation. Therefore, we could not verify the matrix response.

DARPA Comments on Intrusion Detection Software and Firewalls. DARPA stated that the report sections on Intrusion Detection Software and Firewalls contained incorrect statements, adding:

The DoDIG requested specific documentation in writing. Documentation was provided to the DoDIG that details boundary protections, specifically in the form of firewalls, intrusion detection systems, and network topology in place to support protection of the DMSS from external threats. These systems have been in place since DARPA funded research and development of these technologies in the early 1990s.

Audit Response. We requested intrusion detection software and firewall documentation as of August 2001 to verify the DMSS data provided in the matrix. The intrusion detection software and firewall documentation DARPA provided us was dated after August 1, 2001.

DARPA Comments on Red and Blue Team Assessment. DARPA stated that the report section on Red and Blue Team Assessment was incorrect. DARPA stated, “The blue team assessment was performed and documented in 2002. The independent vulnerability assessment was performed February 8, 2000, as stated in the report.”

Audit Response. DARPA responded in the matrix that DMSS had a blue team assessment performed on February 8, 2000. DARPA provided a document described as documentation of the February 8, 2000, blue team assessment. In its comments, DARPA states that an independent vulnerability assessment, not a blue team assessment, was performed on that date. In keeping with the clarification, we have revised the report to state that the DARPA matrix answer showing that a blue team assessment was done in February 2000 was incorrect.

DARPA Comments on Connections. DARPA stated the report section on Connections was incorrect. DARPA stated that DMSS is connected to a larger backbone network (the Internet), for which ASD(C³I) granted a waiver.

Audit Response. We have revised the report to state that the DARPA matrix answer was correct. We request that DARPA provide documentation of the ASD(C³I) waiver in response to the final report.

Site Operational Review

DARPA Comments on Segregation of Duties. DARPA disagreed with the report's statement that key information assurance staff positions were not aligned in a way that ensures segregation of duties and the required checks and balances. DARPA stated:

DITSCAP leaves the determination of proper checks and balances to the discretion of the Component. Further, DARPA has ensured segregation of duties with checks and balances through a CIO [Chief Information Officer] policy memorandum and separation of responsibilities guidance provided to the DoDIG.

Audit Response. Section E3.3.3.6. of the DITSCAP states, "The DAA, the CA [certification authority], the program manager, and the user representative each represent different views and as such provide the checks and balances to ensure the minimum-security requirements are met." The documentation provided by DARPA indicated that the DAA and the certification authority were the same person.

DARPA Comments on Key Information Assurance Staff Positions. DARPA stated that the report is incorrect in stating that DARPA did not formally appoint three of the four key information assurance staff positions required to ensure checks and balances during the certification process. DARPA stated:

The DoDIG is incorrect in stating that these positions are required during the certification process. DITSCAP requires only that individuals be identified, which DARPA did early in the process. Further, while checks and balances are required, they are not necessarily embodied in these positions, as the choice and implementation of checks and balances is under Component discretion. DITSCAP "allows these four managers to tailor . . . efforts to the particular mission . . . of the system." The three key positions were also

documented at the time of the formal accreditation signing (which for DARPA was September 6, 2002); formal appointment is not required by DITSCAP.

Audit Response. Sections E3.3.3.4. and E4.1.1.1. of the DITSCAP states that the key roles in the DITSCAP certification and accreditation process are the system program manager, the DAA, certification authority, and user representative. Further, the DITSCAP requires that appointments to those key roles be made during the first phase of the certification and accreditation process. The DITSCAP allows tailoring of the certification and accreditation process to suit system requirements. For example, combining phases of the certification and accreditation process may be appropriate for modifying an existing information system. However, all phases of certification and accreditation, as shown in Table E4-1 of the DITSCAP, clearly define roles and responsibilities throughout the process for each of the four key roles.

DARPA Comments on Operational Chain of Command. DARPA stated that the report was incorrect in stating that the DAA was not within the operational chain of command as required by the DITSCAP.

Audit Response. Section E4.2.1. of the DITSCAP states, “The DAA should be a senior member of the operational chain-of-command where the system is operating.” According to the DARPA Office of Management Operations Information Assurance Policy, “The IRD [Information Resources Directorate] provides general computing resources for the DARPA enterprise networks, including its IA [Information Assurance] functions, consisting of the physical infrastructure (equipment, cabling and software) and support services needed for acquisition, development, operations, maintenance and security.” The policy also states, “The Information Assurance office, under S&ID [Security and Intelligence Directorate], provides IA policy, IA technical assistance, IA independent verification and validation, and oversight of DARPA IS [information system] resources.” The DARPA DAA was the Director of the Security and Intelligence Directorate rather than an official from the DARPA Information Resources Directorate, which handles operations.

DARPA Comments on Contractor Clearances. DARPA stated that the report was incorrect in stating that DARPA did not provide support that it had verified that contractors working on the system had proper security clearances. DARPA stated:

The DARPA security control system contains all clearance data for all users of the DMSS. Reports of these data can be generated at any time and could have easily been made available by DARPA.

Audit Response. Security clearance levels are not specifically addressed in the matrix. As a result, DARPA did not provide any supporting documentation that it had verified contractor personnel security clearances prior to gaining access to DMSS. A DARPA official agreed to obtain documentation on personnel but did not provide that documentation.

DARPA Comments on Information Security Operational Controls. DARPA took strong exception to the report statement that DARPA may not have adequate information security operational controls, stating:

DARPA's controls go far beyond those required. The proof that those controls safeguard DARPA's information is in independent assessments of the strength of our protections, most recently in the form of a blue team exercise in which no compromises of our system were made.

Audit Response. We concluded that DARPA may not have adequate information security operational controls in place because, as stated in the report:

- the key DARPA information assurance staff positions were not aligned in a way that ensures segregation of duties and the required checks and balances in the DITSCAP for DMSS;
- DARPA did not formally appoint three of the four key information assurance staff positions required to ensure checks and balances during the certification process;
- the DAA was not within the operational chain of command, as the DITSCAP requires; and
- DARPA did not provide support that it had verified that the contractors working on the system had proper security clearances.

DITSCAP Guidance

DARPA Comments on DITSCAP Guidance. DARPA nonconcurred with the report statement that the DITSCAP requires the four key information assurance staff positions to be appointed during the first phase of the certification process. DARPA stated:

DoD 8510.1-M, DITSCAP Application Manual, in Section C3.4.3.2.1, "DITSCAP Phase I Activities," clearly states "Identify the Agency or organization that will serve as the DAA, Certifier, and user representative. Identify individuals and their responsibilities in the C&A [certification and accreditation] process." There is no requirement for appointment. DARPA identified individuals for those key positions, but did not appoint the program manager or user representative until the formal accreditation.

Audit Response. Section E4.2.1.1. of the DITSCAP states that the key parties throughout the DITSCAP are the system program manager, the DAA, the certification authority, and the user representative. Further, the DITSCAP requires that appointments to those key roles be made during the first phase of the certification and accreditation process. All phases of certification and accreditation, as shown in Table E.4-1 of the DITSCAP, clearly define roles and responsibilities throughout the process for each of the four key roles.

Results of Review

DARPA Comments on Alignment of Staff Positions. In response to the report statement that information assurance staff positions were not aligned in a way that would ensure segregation of duties necessary for the checks and balances to ensure minimum security requirements for DMSS, DARPA stated:

This statement is incorrect and misleading. The report makes an implicit assumption that there is only one correct way for Components to ensure segregation of duties with proper checks and balances. DITSCAP leaves the determination of proper checks and balances to the discretion of the Component.

Audit Response. Section E3.3.3.6. of the DITSCAP states, “The DAA, the CA [certification authority], the program manager, and the user representative each represent different views and as such provide the checks and balances to ensure the minimum-security requirements are met.” The documentation provided by DARPA indicated that the DAA and the certification authority were the same person.

DARPA Comments on Formal Appointments. DARPA nonconcurred with the report statement that three of the four key information security staff positions had not been formally appointed. DARPA stated:

This statement is misleading. It implies that these positions are required during the certification process. As stated above, DoD 8510.1-M, DITSCAP Application Manual, in Section C3.4.3.2.1, “DITSCAP Phase I Activities,” clearly states, “Identify the Agency or organization that will serve as the DAA, Certifier, and user representative. Identify individuals and their responsibilities in the C&A [certification and accreditation] process.” There is no requirement for appointment. DARPA identified individuals for those key positions, but did not appoint the program manager or user representative until the formal accreditation.

Audit Response. Section E4.1.1.1. of the DITSCAP states that the key roles in the DITSCAP certification and accreditation process are the system program manager, the DAA, certification authority, and user representative. The DITSCAP also requires that appointments to those key roles must be made during the first phase of the certification and accreditation process. All phases of certification and accreditation, as shown in Table E4-1 of the DITSCAP, clearly define roles and responsibilities throughout the process for each of the four key roles.

DARPA Comments on the DAA. DARPA nonconcurred with the report statement that the DAA for DARPA automated information systems was the Director of the Security and Intelligence Directorate rather than an official from the operational chain of command, such as an official from the DARPA Information Resources Directorate. DARPA stated:

This statement is incorrect. The DAA is, in fact, within the operational chain of command. DARPA maintains a matrixed command structure

for network operations. The DAA plays a critical function in that operation. In fact, the network cannot operate without the expressed consent of the DAA. The DAA has the operational power to shut down the network at any time.

Audit Response. Section E4.2.1. of the DITSCAP states, “The DAA should be a senior member of the operational chain-of-command where the system is operating.” According to the DARPA Office of Management Operations Information Assurance Policy, “The IRD [Information Resources Directorate] provides general computing resources for the DARPA enterprise networks, including its IA [information assurance] functions, consisting of the physical infrastructure (equipment, cabling and software) and support services needed for acquisition, development, operations, maintenance and security.” The policy also states, “The Information Assurance office, under S&ID [Security and Intelligence Directorate], provides IA [information assurance] policy, IA technical assistance, IA independent verification and validation, and oversight of DARPA IS [information systems] resources.” The DARPA DAA was the Director of the Security and Intelligence Directorate rather than an official from the DARPA Information Resources Directorate, which handles operations. DARPA did not provide documentation on the matrixed command structure.

DARPA Comments on Contractor Clearances. DARPA stated that the report was misleading in making the statement that DARPA did not provide supporting documentation that it had verified contractor personnel security clearances before granting contractors access to DMSS. DARPA stated:

In fact, the DoDIG never asked for such data. The DARPA security control system contains all clearance data for all users of the DMSS. Reports of these data can be generated at any time and could have easily been made available.

Audit Response. Security clearance levels are not specifically addressed in the matrix. As a result, DARPA did not provide any supporting documentation that it had verified contractor personnel security clearances before granting contractors access to DMSS. Although a DARPA official agreed to provide the support on the clearance levels of contractor personnel, that official did not provide the documentation.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)/Chief Financial Officer
Deputy Chief Financial Officer
Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Director, Defense-Wide Information Assurance Program

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Advanced Research Projects Agency
Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Inspector General, Defense Information Systems Agency
Director, Defense Logistics Agency

Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform

Defense Advanced Research Projects Agency Comments



DEFENSE ADVANCED RESEARCH PROJECTS AGENCY
3701 NORTH FAIRFAX DRIVE
ARLINGTON, VA 22203-1714

OCT 3 2002

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDITING,
DEPARTMENT OF DEFENSE INSPECTOR GENERAL (DoDIG)
DIRECTOR, READINESS AND LOGISTICS SUPPORT
DIRECTORATE, DoDIG

SUBJECT: Report on Government Information Security Reform (GISR) Act Implementation:
Defense Advanced Research Projects Agency (DARPA) Management Support
System (Project No. D2002LD-0101)

We have reviewed the subject draft report of August 22, 2002, and appreciate this opportunity to respond with comments, which are attached and follow the format requested in the cover memorandum. We request you publish these comments in their entirety with the final report.

We are particularly concerned that the Executive Summary concludes, "As a result, the DARPA Management Support System may not have adequate information security operational controls that ensure sensitive information is safeguarded." DARPA takes strong exception to this statement. DARPA's controls go far beyond those required. We recently had an independent penetration test in which no compromise of our system was made.

I believe our DARPA Management Support System (DMSS) is among the best protected, best designed, and best managed systems in the Department. We have survived viruses, worms, denial-of-service attacks, and other problems with little or no effect. Your report does not reflect this, but rather paints a far different picture.

We take exception to certain conclusions and statements included in the draft report. In a number of instances, the draft states that the DoDIG could not verify DARPA's response on the GISR data matrix because DARPA did not provide sufficient information. Our records show that we responded with materials for every item on the list of requested data. Moreover, we provided a rebuttal of this and other points in response to the discussion draft of this report.

We nonconcur with the majority of the findings throughout the report, and we provide specific responses to all. The Executive Summary states that DARPA answered 5 of the 32 GISR matrix questions incorrectly and did not provide documentation for 8 others. Two of the five "incorrect" answers were trivial or open to interpretation (use of "July 15" vice "July 17" and use of "Yes" vice "N/A"). For the remaining three, our "Yes" responses are, in fact, correct and the DoDIG has incorrectly assessed the data with which they worked. In the case of the eight matrix items for which DoDIG states that DARPA did not provide supporting documentation, appropriate documentation was, in fact, provided in accordance with the written list provided by the DoDIG auditors. If the documentation was insufficient for the auditors' purposes, they failed to inform us.

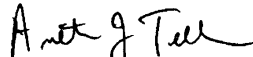
The Summary states we did not make three of four required key staff appointments. The DoD Information Technology Secret Certification and Accreditation Process (DITSCAP) does not require formal appointment of these positions during Phase I of certification work; only identification is required. DARPA identified individuals for these positions in Phase I, all of whom performed in their roles throughout the certification process. The Summary further states the Designated Approving Authority (DAA) position was not within the operational chain of command. This is not correct. The position is not only within the chain of command, but also has the power to shut down the entire network at any time.

The Summary also states these positions were not aligned as required by DITSCAP, although DITSCAP leaves alignment to the Components and "allows these four managers to tailor . . . efforts to the particular mission . . . of the system." DARPA has ensured segregation of duties with checks and balances through a Chief Information Officer (CIO) policy memorandum and separation of responsibilities guidance, both provided to the DoDIG. These documents show that information assurance is completely independent of network operations and has dotted-line responsibility directly to the DARPA CIO.

Finally, the Summary states DARPA did not verify that contractors on the system have proper security clearances. In fact, the DoDIG never asked for such data. Rather, they asked for logs detailing accesses by individual badge holders at perimeter doors. Although the auditors were told all such badge holders possess Secret clearances, they did not ask for verifying data, which is kept current and available in our Security Information Management System.

The report's three recommendations stem directly from the findings on key staff and clearance documentation. DARPA nonconcurs for the reasons stated above.

In accordance with your instructions, this response is being sent via email and in hardcopy. Questions regarding this response may be addressed to my point of contact, Mr. Brian Sosdian, 703-696-2418, bsosdian@darpa.mil.


Anthony J. Tether
Director

Attachment:
As stated

**AGENCY RESPONSE TO DRAFT REPORT
of the
Office of the Inspector General of the Department of Defense**

Project No. D2002LD-0101

September 20, 2002

**Government Information Security Reform Act Implementation:
Defense Advanced Research Projects Agency
Management Support System**

Defense Advanced Research Projects Agency (DARPA) disagrees with a number of statements made by the Office of the Inspector General of the Department of Defense (DoDIG) in its Draft Report dated August 22, 2002. DARPA found problems in the Report's Summary, Findings, and Collection Matrix audit results. Some statements are incorrect; many are misleading. This response delineates DARPA's position on each of the issues raised by the DoDIG in the order in which they appear and provides information to correct each.

EXECUTIVE SUMMARY

Results (page i)

REPORT STATES: "DARPA answered 5 of the 32 collection matrix data fields incorrectly."

DARPA RESPONSE: **Nonconcur.** Answers to 2 of the 32 fields are technically incorrect, but of no consequence. One of the two answers is a minor clerical error (July 15 vice July 17; note this is referred to as "essentially correct" on page 6 of the Draft Report under "Interim Certification Date") and the other is a "Yes" instead of a more precise "N/A." The other three fields are answered correctly and appropriately. DARPA answered "Yes" to the question "Accreditation under DITSCAP?" This question asks if DITSCAP is the framework under which accreditation is developed, not whether that accreditation has been completed (which is asked separately above it.) DARPA was correct to respond "Yes" in that DARPA was using DITSCAP as the basis for all accreditation and certification work. Second, DoDIG found DARPA's "Yes" answer to the question "Contingency Plans in place?" incorrect, citing "That plan addressed only 2000 activities and did not address contingency operations in a broader context." While the plan had been developed for Year 2000 (Y2K) purposes, it provides checks, tests and restoration procedures for every foreseeable system failure whether or not a failure might be caused by Y2K problems, fire, flood, or malicious intent. Furthermore, the DoDIG made this assessment after receiving less than 1 percent of DARPA's Y2K documentation. DARPA's "Yes" response was fully appropriate. Third, DoDIG claims DARPA's answer of "December 30, 1999" is incorrect in answering the question "Date contingency plans last exercised?" citing the same reason as above, that it "was performed for 2000 concerns and not applicable to current conditions." As indicated above, *the contingency plan is wholly adequate* for any contingency. DARPA's answer is correct.

REPORT STATES: "DARPA did not provide documentation that supported 8 of the 32 responses."

DARPA RESPONSE: **Nonconcur.** DARPA provided all documentation requested by DoDIG, including documentation for these eight matrix items. DARPA's selection of items to give to DoDIG was based on a list of required documents that the auditors provided to DARPA. DARPA responded to all items on that list and did not receive notification of documentation shortfalls.

REPORT STATES: "... the key DARPA information assurance staff positions were not aligned in a way that ensures segregation of duties and the required checks and balances in the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) for the DMSS."

DARPA RESPONSE: **Nonconcur.** In fact, DITSCAP leaves the determination of proper checks and balances to the discretion of the Component. Further, DARPA has ensured segregation of duties with checks and balances through a Chief Information Officer (CIO) policy memorandum and separation of responsibilities guidance provided to DoDIG. These documents show that information assurance is completely independent of the network operations and has dotted-line responsibility directly to the DARPA CIO.

REPORT STATES: "DARPA did not formally appoint three of the four key information assurance staff positions required to ensure the appropriate checks and balances during the certification process."

DARPA RESPONSE: **Nonconcur.** The DoDIG is incorrect in stating that these positions are required during the certification process. DITSCAP requires only that individuals be identified, which DARPA did early in the process. Further, while checks and balances are required, they are not necessarily embodied in these positions, as the choice and implementation of checks and balances is under Component discretion. DITSCAP "allows these four managers to tailor ... efforts to the particular mission ... of the system." The three key positions were also documented at the time of the formal accreditation signing (which for DARPA was September 6, 2002); formal appointment is not required by DITSCAP.

REPORT STATES: "... the designated approving authority was not within the operational chain of command, as the DITSCAP requires."

DARPA RESPONSE: **Nonconcur.** This statement is incorrect. The Designated Approving Authority (DAA) is, in fact, within the operational chain of command. DARPA maintains a matrixed command structure for network operations. The DAA plays a critical function in that operation. In fact, the network cannot operate without the expressed consent of the DAA. The DAA has the operational power to shut down the network at any time.

REPORT STATES: "DARPA did not provide support that they had verified that the contractors working on the system had proper security clearances."

DARPA RESPONSE: **Nonconcur.** This statement is misleading. In fact, the DoDIG never asked for such data. The DARPA security control system contains all clearance data for all users of the DMSS. Reports of these data can be generated at any time and could have easily been made available. The DoDIG never requested such data. They requested and received a

report from DARPA's door access system showing all physical accesses by individuals to DARPA-controlled spaces on two specific dates.

REPORT STATES: "As a result, the DARPA Management Support System may not have adequate information security operational controls that ensure sensitive information is safeguarded."

DARPA RESPONSE: **Nonconcur**. DARPA takes strong exception to this statement. DARPA's controls go far beyond those required. The proof that those controls safeguard DARPA's information is in independent assessments of the strength of our protections, most recently in the form of a penetration test in which no compromises of our system were made. Further, without exception, in virus, worm, denial-of-service, and other wide-spread attacks reported in the media, DARPA has experienced little or no effect.

FINDINGS

Mission and System Information (page 4)

Contract Support

REPORT STATES: "In September 2001, DARPA contracted for DMSS hardware, software, and systems support."

DARPA RESPONSE: **Nonconcur**. This is incorrect. The DMSS is a legacy system and has existed since the early 1980s. It and other Information Technology (IT) assets were transferred to the extant contractor under a modified managed services contract awarded in April 2001.

Data Collection Matrix (pages 5-12)

Identifying Information

REPORT STATES: "... the identifying information in the matrix was incorrectly reported because DMSS was not a mission-critical system but a mission-essential system ..."

DARPA RESPONSE: **Concur**. This is a reporting error that was not caught before release.

Accreditation Information

Accreditation Date

REPORT STATES: "DARPA was requested to provide the date that an accreditation process accredited DMSS."

DARPA RESPONSE: **Concur**. DARPA left the response blank since it plans to accredit the DMSS by September 30, 2002.

Accreditation Method

REPORT STATES: "DARPA responded in the matrix that they were using DITSCAP to certify and accredit the DMSS. We verified that the response was incorrect and that the DMSS was following DITSCAP procedures, but DARPA should have responded 'no' to the question because as of August 1, 2001, DMSS was not accredited."

DARPA RESPONSE: **Nonconcur.** DARPA's "Yes" answer was correct. The matrix question is "Accreditation under DITSCAP?" This question asks if DITSCAP is the framework under which accreditation is developed, not whether that accreditation has been completed (which is asked separately above it). DARPA is correct to respond "Yes" in that DARPA was using DITSCAP as the basis for all accreditation and certification work.

Certification and Accreditation Documentation

REPORT STATES: "Since then, DARPA has developed an in-process SSAA . . . we identified the documents as in-process to indicate that they are not final documents, but are apparently being used by DARPA."

DARPA RESPONSE: **Nonconcur.** The DoDIG term "in-process" is misleading and does not convey the true state of the accreditation documents given to the DoDIG. Those documents were complete and reviewed by senior management at the time they were written. Because the DMSS is a dynamic system, with frequent (often weekly) changes, the supporting documents are under constant revision. They could not, by definition, be "approved" until formal accreditation. They were as fully operational before the accreditation as after. Accreditation occurred September 6, 2002.

Assessment Criteria Information

Access Controls

REPORT STATES: "DARPA did not provide documentation that supported the 'yes' response for having access controls in place as of August 1, 2001. As a result, we could not verify the response."

DARPA RESPONSE: **Nonconcur.** This is an incorrect statement. The DoDIG requested specific documentation in writing. DARPA provided that documentation and did not receive any response stating such documentation was insufficient for their needs. The documentation provided to the DoDIG was DITSCAP documentation dated after August 1, 2001, which details the physical, technical, and administrative controls in place to protect the DMSS. Similar controls have been in place since the initial implementation of the DMSS in the early 1980s. The DITSCAP process creates operational documentation that, by nature, is continually revised, versioned, and re-dated. Thus, the documentation date does not reflect the implementation date. If the DoDIG had requested documentation beyond its original request, DARPA would have supplied other documentation showing the controls in place on and before August 1, 2001. No such request was received.

System Life-Cycle Plan

REPORT STATES: "We confirmed that when DARPA submitted the matrix data as of August 1, 2001, they had not developed a DMSS System Life-Cycle Plan. However, since that time, DARPA has a system life-cycle requirement that called for hardware and software to be replaced when or before either reaches 24 months of age."

DARPA RESPONSE: **Nonconcur**. This is not completely correct and is somewhat misleading. DARPA has always had a life-cycle requirement for refreshment of DMSS components. As of April 2001, the effective date of the latest contract for DMSS support, this requirement was 24 months. Prior to that, it was 36 months. DARPA responded "No" to the matrix question because a formal life-cycle plan containing all definitional components of such plans is not appropriate for the DMSS. The refresh requirement is the appropriate mechanism to maintain system currency.

Revised

System Security Plan

REPORT STATES: "DARPA responded in the matrix that a DMSS System Security Plan was not completed . . . since that time, DARPA developed a DMSS System Security Plan."

DARPA RESPONSE: **Concur**

Personnel Security Measures

REPORT STATES: "DARPA did not provide documentation that supported the 'yes' response for having access controls in place as of August 1, 2001. As a result, we could not verify the response."

DARPA RESPONSE: **Nonconcur**. This is an incorrect statement. The DoDIG requested specific documentation in writing. DARPA provided that documentation and did not receive any response stating such documentation was insufficient for their needs. The documentation provided to the DoDIG was DITSCAP documentation dated after August 1, 2001, which details the controls related to personnel security that were in place to protect the DMSS. Similar controls have been in place since the initial implementation of the DMSS in the early 1980s. The DITSCAP process creates operational documentation that, by nature, is continually revised, versioned, and re-dated. Thus, the documentation date does not reflect the implementation date. If the DoDIG had requested documentation beyond its original request, DARPA would have supplied other documentation showing the controls in place on August 1, 2001. No such request was received.

Physical Security Controls

REPORT STATES: "We verified that physical security controls were in place. An electronic card access system controlled primary access to the DARPA office suites. Since August 2001, other physical security controls were implemented."

DARPA RESPONSE: **Nonconcur**. This finding is misleading. The wording implies that on August 1, 2001, DARPA had only its electronic card access

Revised

system in place as a physical security control. It implies that the other controls were added after August 1, 2001. All security measures mentioned here, with the exceptions of armed (vs. unarmed) guards and an on-station Arlington County police officer, have been in place at DARPA for many years. These facts were conveyed to the DoDIG during their on-site review.

Administrative Controls

REPORT STATES: "DARPA did not provide documentation that supported the 'yes' response as of August 1, 2001. As of August 1, 2001, we verified that DARPA had a help desk, but we could not verify that DARPA had established audit trails."

DARPA RESPONSE: **Nonconcur.** These are incorrect statements. The DoDIG requested specific documentation in writing. DARPA provided that documentation and did not receive any response stating such documentation was insufficient for their needs. The documentation provided to the DoDIG was DITSCAP documentation dated after August 1, 2001, which indicates that administrative controls were in place. Similar controls have been in place since the initial implementation of the DMSS in the early 1980s. The DITSCAP process creates operational documentation that, by nature, is continually revised, versioned, and re-dated. Thus, the documentation date does not reflect the implementation date. If the DoDIG had requested documentation beyond its original request, DARPA would have supplied audit logs and other documentation showing the controls in place on and before August 1, 2001. No such request was received.

Contingency Plans

REPORT STATES: "We verified that DARPA had a contingency plan for 2000; however, DARPA should have responded 'no' because the 'yes' response was based on the 2000 Contingency Plan."

DARPA RESPONSE: **Nonconcur.** This statement is incorrect. There is no basis in fact for saying that a Y2K contingency plan is not appropriate for future use. In fact, the DARPA Y2K contingency exercise was a monumental effort for such a small agency and system. Every aspect of the system was examined, analyzed, and documented, and every effort was made to contemplate all possibilities for disruption. That documentation, with its detailed procedures for responding to a wide range of disruptions, including total system replacement, was a highly useful contingency plan on August 1, 2001.

REPORT STATES: "That plan discussed two DARPA mission-essential systems: the main DARPA building and the financial information system. The plan does not mention DMSS or similar local area network system that predated DMSS."

DARPA RESPONSE: **Nonconcur.** This statement is incorrect. There is only one DARPA system, which is the mission-essential DMSS, so named in the DoD Y2K Data Base, which preceded the DoD IT Registry. The voluminous plan

discusses nothing but the DMSS, DARPA's single local area network, including all attachments and peripherals.

REPORT STATES: "We verified that the contingency plan was exercised in the December 1999 time frame. However, DARPA should not have answered with a date because the exercise was based on a year 2000 contingency plan."

DARPA RESPONSE: **Nonconcur**. This statement is incorrect. As indicated above, there is no basis for categorically stating the plan should not have been used for an exercise just because it was developed for Y2K concerns. In fact, it is as good and appropriate a plan as could have been used at the time, with no additional costs incurred.

REPORT STATES: "Furthermore, the 2000 Contingency Plan exercise focused only on interruptions for 2000."

DARPA RESPONSE: **Nonconcur**. This is an incorrect statement. Again, as indicated above, the 2000 Contingency Plan provides detailed procedures covering the widest possible range and degree of disruptions, whether those disruptions might be caused by utility failures, fire, flood, malicious intent, or other problems. The DoDIG based its report on less than 1 percent of the Y2K documentation. The DoDIG was informed of this, and that additional documentation would be provided if requested. No such request was received.

Hardware and Software Maintenance Plans

REPORT STATES: "However, DARPA did not provide documentation that supported the 'yes' response as of August 1, 2001. As a result, we could not verify the response."

DARPA RESPONSE: **Nonconcur**. This is an incorrect statement. The DoDIG requested specific documentation in writing. DARPA provided that documentation and did not receive any response stating such documentation was insufficient for their needs. The documentation provided to the DoDIG was DITSCAP documentation dated after August 1, 2001, which details hardware and software evaluation, conformance and conflict testing, version control and update procedures. Similar procedures have been in place since the initial implementation of the DMSS in the early 1980s. The DITSCAP process creates operational documentation that, by nature, is continually revised, versioned, and re-dated. Thus, the documentation date does not reflect the implementation date. If the DoDIG had requested documentation beyond its original request, DARPA would have supplied other documentation showing the controls in place on and before August 1, 2001. No such request was received.

Data Integrity Process

REPORT STATES: "DARPA did not provide documentation that supported the 'yes' response as of August 1, 2001. As a result, we could not verify the response."

DARPA RESPONSE: **Nonconcur**. This is an incorrect statement. The DoDIG requested specific documentation in writing. DARPA provided that

documentation and did not receive any response stating such documentation was insufficient for their needs. The documentation provided to the DoDIG was DITSCAP documentation dated after August 1, 2001, which details an in-place data integrity process that protects DMSS data from accidental or malicious alteration or destruction and is used to provide assurances to DARPA users that the information meets their expectations of quality and integrity. Similar procedures have been in place since the initial implementation of the DMSS in the early 1980s. The DITSCAP process creates operational documentation that, by nature, is continually revised, versioned, and re-dated. Thus, the documentation date does not reflect the implementation date. If the DoDIG had requested documentation beyond its original request, DARPA would have supplied other documentation showing the controls in place on and before August 1, 2001. No such request was received.

Security Incident Response Plan

REPORT STATES: "DARPA did not provide documentation that supported the 'yes' response as of August 1, 2001. As a result, we could not verify the response."

DARPA RESPONSE: **Nonconcur.** This is an incorrect statement. The DoDIG requested specific documentation in writing. DARPA provided that documentation and did not receive any response stating such documentation was insufficient for their needs. The documentation provided to the DoDIG details our security incident response plan that is in place to protect the DMSS from adverse events that could cause a failure of security mechanisms or when an attempted breach of these mechanisms occurs. If the DoDIG had requested documentation beyond its original request, DARPA would have supplied other documentation showing the plan in place. No such request was received.

Operations and Assessments Interest Items

Network Protections

Intrusion Detection Software/Firewalls

REPORT STATES: "DARPA did not provide documentation that supported the 'yes' responses as of August 1, 2001. As a result, we could not verify the responses."

DARPA RESPONSE: **Nonconcur.** This is an incorrect statement. The DoDIG requested specific documentation in writing. Documentation was provided to the DoDIG that details boundary protections, specifically in the form of firewalls, intrusion detection systems, and network topology in place to support protection of the DMSS from external threats. These systems have been in place since DARPA funded research and development of these technologies in the early 1990s. Today, DARPA employs state-of-the-art, redundant firewalls. DARPA provided that documentation and did not receive any response stating such documentation was insufficient for DoDIG needs. If the DoDIG had

requested documentation beyond its original request, DARPA would have supplied alternate or additional documentation showing the firewalls in place. No such request was received.

Vulnerabilities

Red and Blue Team Assessment

REPORT STATES: "DARPA responded in the matrix that DMSS had a blue team assessment performed on February 8, 2000."

DARPA RESPONSE: **Nonconcur**. This statement is incorrect. The blue team assessment was performed and documented in 2002. The independent vulnerability assessment was performed February 8, 2000, as stated in the report.

Revised

Connections

REPORT STATES: "DARPA responded in the matrix that the DMSS interface connections were approved. DARPA should have responded 'NA' [Not Applicable] because they did not have an unclassified connection for which approval was required."

DARPA RESPONSE: **Nonconcur**. This statement is incorrect. DARPA is directly connected to a larger backbone network (the Internet) through redundant Internet service providers. This connection is based on a waiver granted by the Assistant Secretary of Defense (Command, Control Communications and Intelligence) (ASD(C3I)) to exempt DARPA from connection to the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet), a DoD requirement. Therefore DARPA does have connection approval to connect to a larger backbone network.

Revised

Information Assurance Vulnerability Alert

REPORT STATES: "DARPA responded in the matrix that DMSS was fully information assurance vulnerability alert compliant."

DARPA RESPONSE: **Concur**.

Vulnerability Analysis and Assistance Program

REPORT STATES: "We confirmed that the DARPA response was appropriate as of August 1, 2001 ..."

DARPA RESPONSE: **Concur**.

Assessments

REPORT STATES: "DARPA responded in the matrix that none of these assessments had been performed."

DARPA RESPONSE: **Concur**.

Site Operational Review (page 12)

REPORT STATES: “However, the key DARPA information assurance staff positions were not aligned in a way that ensures segregation of duties and the required checks and balances in the DITSCAP for the DMSS.”

DARPA RESPONSE: **Nonconcur.** This statement is incorrect. DITSCAP leaves the determination of proper checks and balances to the discretion of the Component. Further, DARPA has ensured segregation of duties with checks and balances through a CIO policy memorandum and separation of responsibilities guidance provided to the DoDIG. These documents show that information assurance is completely independent of the network operations and has dotted-line responsibility directly to the DARPA CIO.

REPORT STATES: “Furthermore, DARPA did not formally appoint three of the four key information assurance staff positions required to ensure checks and balances during the certification process.”

DARPA RESPONSE: **Nonconcur.** The DoDIG is incorrect in stating that these positions are required during the certification process. DITSCAP requires only that individuals be identified, which DARPA did early in the process. Further, while checks and balances are required, they are not necessarily embodied in these positions, as the choice and implementation of checks and balances is under Component discretion. DITSCAP “allows these four managers to tailor . . . efforts to the particular mission . . . of the system.” The three key positions were also documented at the time of the formal accreditation signing (which for DARPA was September 6, 2002); formal appointment is not required by DITSCAP.

REPORT STATES: “Also, the DAA was not within the operational chain of command, as the DITSCAP requires.”

DARPA RESPONSE: **Nonconcur.** This statement is incorrect. The DAA is, in fact, within the operational chain of command. DARPA maintains a matrixed command structure for network operations. The DAA plays a critical function in that operation. The network cannot operate without the expressed consent of the DAA. The DAA has the operational power to shut down the network at any time.

REPORT STATES: “Further, DARPA did not provide support that they had verified that the contractors working on the system had proper security clearances.”

DARPA RESPONSE: **Nonconcur.** This statement is incorrect. The DoDIG never asked for such data. The DARPA security control system contains all clearance data for all users of the DMSS. Reports of these data can be generated at any time and could have easily been made available by DARPA. The DoDIG never requested such data. They requested and received a report from DARPA’s door access system showing all physical accesses by individuals to DARPA controlled spaces on two specific dates.

REPORT STATES: “As a result, DMSS may not have adequate information security operational controls that ensure sensitive information is safeguarded.”

DARPA RESPONSE: **Nonconcur.** DARPA takes strong exception to this statement. DARPA’s controls go far beyond those required. The proof that those controls safeguard

DARPA's information is in independent assessments of the strength of our protections, most recently in the form of a blue team exercise in which no compromises of our system were made. Further, without exception, in virus, worm, denial-of-service, and other attacks of the past, DARPA has fared far better than any DoD organization known to us and has never suffered significant damage.

DITSCAP Guidance (page 12)

Page 11

REPORT STATES: "... DITSCAP requires that the four key information assurance staff positions [DAA, Certifier, program manager, and user representative] be appointed during the first phase of the certification process."

DARPA RESPONSE: **Nonconcur.** This statement is incorrect. DoD 8510.1-M, DITSCAP Application Manual, in Section C3.4.3.2.1, "DITSCAP Phase I Activities," clearly states "Identify the Agency or organization that will serve as the DAA, Certifier, and user representative. Identify individuals and their responsibilities in the C&A process." There is no requirement for appointment. DARPA identified individuals for those key positions, but did not appoint the program manager or user representative until the formal accreditation.

Results of Review (page 13)

Page 12

REPORT STATES: "The key DARPA information assurance staff positions were not aligned in a way that would ensure segregation of duties necessary for the checks and balances to ensure minimum security requirements for DMSS."

DARPA RESPONSE: **Nonconcur.** This statement is incorrect and misleading. The report makes an implicit assumption that there is only one correct way for Components to ensure segregation of duties with proper checks and balances. DITSCAP leaves the determination of proper checks and balances to the discretion of the Component. DARPA has ensured segregation of duties with checks and balances through a CIO policy memorandum and separation of responsibilities guidance, which DARPA provided to the DoDIG. These documents show that information assurance is completely independent of the network operations and has dotted-line responsibility directly to the DARPA CIO, ensuring checks and balances that are appropriate for DARPA.

REPORT STATES: "According to the list in the System Security Plan (SSP), both the Designated Approving Authority (DAA) and certification authority positions were listed as duties the Director of the Security and Intelligence performed."

DARPA RESPONSE: **Concur with comments.** While this statement is correct, the assignments in question were initially made based on a preliminary interpretation of DITSCAP requirements for these positions. This interpretation has since been revised, and the current version of the SSP shows the certification authority to be the Manager, Information Security, while the DAA remains the Director, Security and Intelligence. This was an administrative change of overall responsibility only. It did not affect the actual performance of detailed tasks under each of these positions. All certification work,

since the beginning of DITSCAP Phase I, was actually performed by the Manager, Information Security. The Manager, Information Security, has dotted-line authority directly from the DARPA CIO, who regularly meets with this manager to ensure the visibility and resolution of any conflict between the Certification Authority and the DAA.

REPORT STATES: "Additionally, DARPA did not formally appoint three of the four key information assurance staff positions."

DARPA RESPONSE: **Nonconcur.** This statement is misleading. It implies that these positions are required during the certification process. As stated above, DoD 8510.1-M, DITSCAP Application Manual, in Section C3.4.3.2.1, "DITSCAP Phase I Activities," clearly states, "Identify the Agency or organization that will serve as the DAA, Certifier, and user representative. Identify individuals and their responsibilities in the C&A process." There is no requirement for appointment. DARPA identified individuals for those key positions, but did not appoint the program manager or user representative until the formal accreditation.

REPORT STATES: "... the DAA for DARPA automated information systems, was the Director of the Security and Intelligence Directorate rather than an official from the operational chain of command such as an official from the DARPA Information Resources Directorate."

DARPA RESPONSE: **Nonconcur.** This statement is incorrect. The DAA is, in fact, within the operational chain of command. DARPA maintains a matrixed command structure for network operations. The DAA plays a critical function in that operation. In fact, the network cannot operate without the expressed consent of the DAA. The DAA has the operational power to shut down the network at any time.

REPORT STATES: "DARPA did not provide us with any supporting documentation that they had verified contractor personnel security clearances prior to granting access to DMSS."

DARPA RESPONSE: **Nonconcur.** This statement is misleading. In fact, the DoDIG never asked for such data. The DARPA security control system contains all clearance data for all users of the DMSS. Reports of these data can be generated at any time and could have easily been made available. The DoDIG never requested such data. They requested and received a report from DARPA's door access system showing all physical accesses by individuals to DARPA-controlled spaces on two specific dates.

Recommendations (page 14)

1. REPORT RECOMMENDS: "Formally appoint a program manager, certification authority, and user representative . . . that are organizationally aligned in a way that will provide checks and balances"

DARPA RESPONSE: **Nonconcur.** DARPA's alignment of information assurance staff positions is correct and appropriate for this organization. It follows DITSCAP requirements by achieving the checks and balances appropriate for DARPA. DITSCAP places the decisions involved in these assignments at the Component level.

2. REPORT RECOMMENDS: “Verify that the certification authority and designated approving authority are separate and independent from each other.”

DARPA RESPONSE: **Nonconcur.** These positions are and have been separate and independent since the initiation of the DITSCAP work. The CIO supervises both positions to ensure independent work, advice, and visibility and resolution of any conflict.

3. REPORT RECOMMENDS: “Properly document the security clearance levels for all of the information systems contract support personnel that have access to the Defense Advanced Research Projects Agency Management Support System.”

DARPA RESPONSE: **Nonconcur.** This documentation has always existed. DARPA will certainly share this documentation with the DoDIG if it is requested. To date, it has not been requested.

Team Members

The Readiness and Logistics Support Directorate, Office of the Assistant Inspector General for Auditing of the Department of Defense prepared this report. Personnel of the Office of the Inspector General of the Department of Defense who contributed to the report are listed below.

Shelton R. Young
Tilghman A. Schraden
Kathryn L. Palmer
Jason T. Steinhart
Susan R. Ryan
Sharon L. Carvalho
Elizabeth L.N. Shifflett